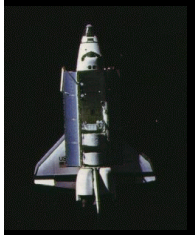
Fault Management Techniques in Human Spaceflight Operations

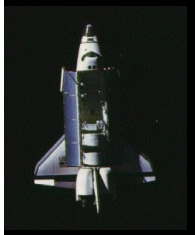
ISHEM Forum 2005

Brian O'Hagan
Alan Crocker
NASA/Johnson Space Center
Mission Operations Directorate



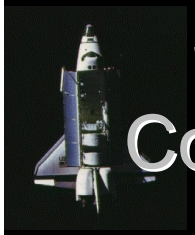
Contents

- Flight Operations Team
- System Architecture Implications
- Operations Processes and Techniques
- Lessons Learned



Flight Operations Team

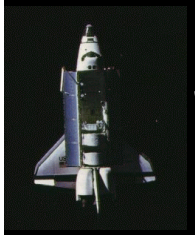
- Crew
  - *Purpose of manned spaceflight*
  - *Conduct Science*
  - *Maintenance*
  - *Response to failures not handled by FDIR/autonomy*
- Flight Control Team (FCT)
  - *Flight Director – Leads FCT and crew*
  - *Capcom – Talks to the crew to insure consistency*
  - *Systems Flight Controllers – System experts, troubleshooting*
  - *Planners – Develop timeline, track consumables, schedule comm*
  - *Trajectory Flight Controllers – Track location and trajectory*
  - *Crew Support – IFM, Crew Health, Surgeon, etc.*



System Architecture Implications

Components of a good failure management design

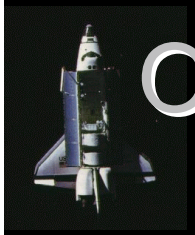
- Fault Prevention
  - *Increase reliability by reducing possible failure modes.*
  - *Operations staffing, training, procedure development is based on what could or will happen.*
- Fault Mitigation
  - *Reduce the impact of a failure through the use of fault tolerance.*
  - *Fault tolerant systems allow the operations team to work around the fault to achieve the mission objectives.*
- Fault Detection
  - *Identification of a failure event through sensor data, built-in test data, and other observed component performance information*
  - *Fault detection should be reliable and convey the importance of the failure. Always work the highest priority events first.*
- Fault Protection
  - *System (automated) response to a fault.*
  - *Fault protection should be autonomous and not require intervention by the crew or FCT if possible.*
- Recovery
  - *Safing of failed systems components and preservation of critical vehicle functions*



System Architecture Implications

Other Factors

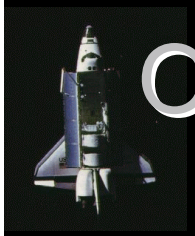
- System complexity
- System interdependencies
- Commonality
- Hardware switch control vs. software control
- Software defects



Operations Processes and Techniques
Roles and Responsibilities

- Crew
  - *Prime for emergency response and other immediate actions*
  - *Only option for In-Flight Maintenance (IFM)*
  - *Typical Size: 2 (Increment Ops) to 7 (Shuttle crew)*

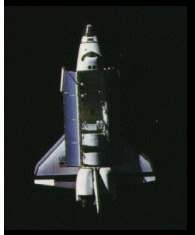
- Flight Control Team
  - *Supports all phases of failure response*
  - *Develops procedures, timeline, documentation*
  - *Develops work-arounds and support the crew for failures*
  - *Has more detailed insight into system than crew displays*
  - *Typical size:15 (ISS Day shift, complex activities) to 40 (Shuttle flight)*
  - *Reduced Staffing: ISS support can be reduced to 6*



Operations Processes and Techniques
Roles and Responsibilities

- External Interfaces
  - Mission Evaluation Room (MER)
    - *Interface between the FCT and ESC*
    - *Works with FCT for anomaly resolution, detailed troubleshooting, provide engineering analysis*
    - *Full staffing for complex periods and assembly flights*
    - *Nominal staffing varies based on activities*
    - *On-call for other periods*
  - Engineering Support Centers (ESC)
    - *On-call for troubleshooting and critical activities*

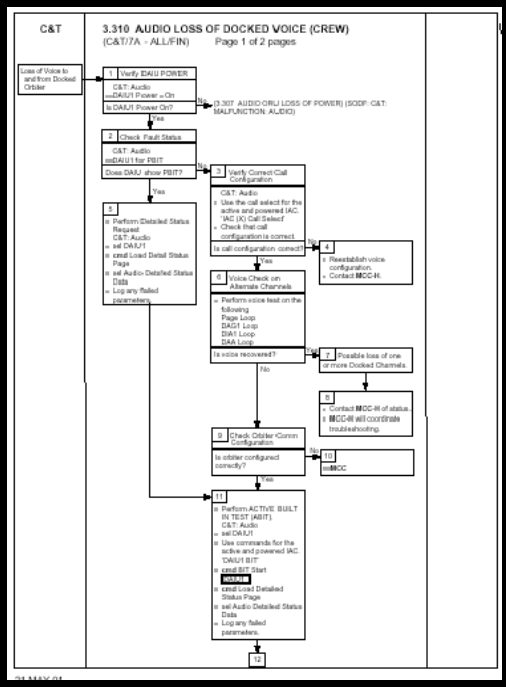
- Training Team
  - *Trains crew*
  - *Trains FCT*
  - *Helps with procedure validation and what-if testing*

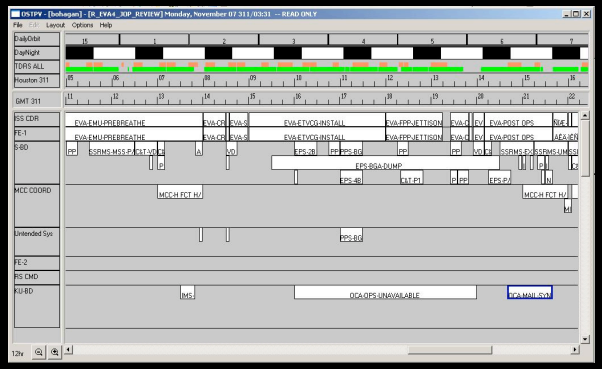


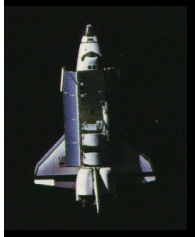
Operations Resources and Tools

Operations Products

- Plans – *Document activities to be performed (Timeline) and any constraints*
- Procedures – *Validated steps necessary to accomplish a given task*
- Flight Rules – *Documented predetermined decisions used to minimize time and effort required to take action in real-time*
- Anomaly Reports – *Track anomalies and their resolutions*



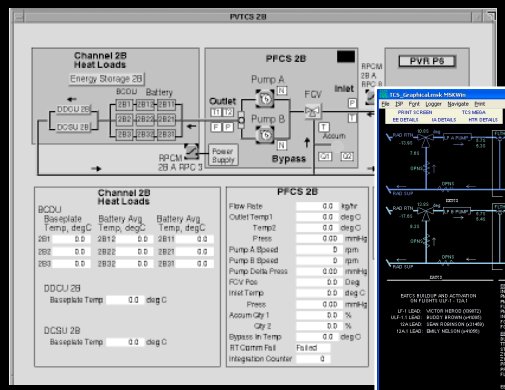


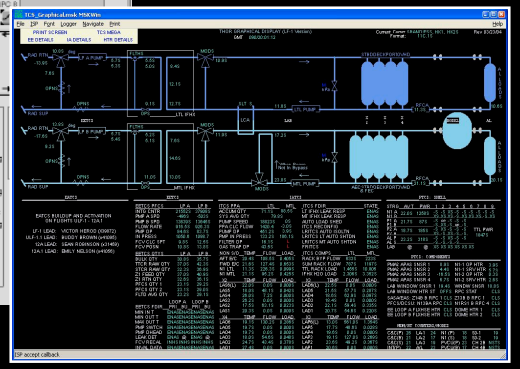


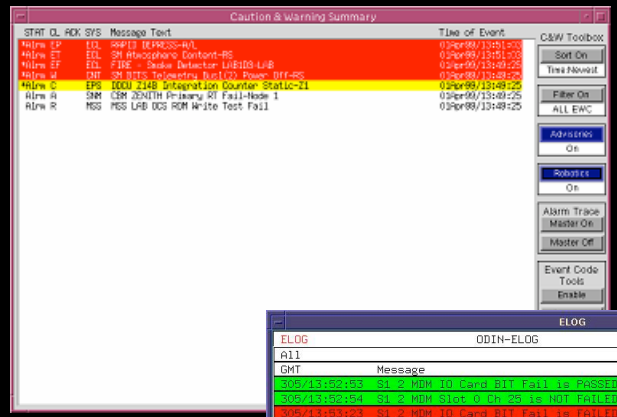
Operations Resources and Tools

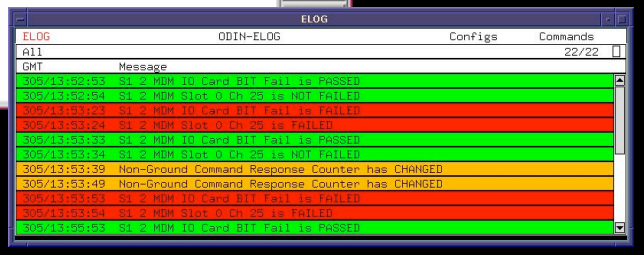
Situational Awareness Tools

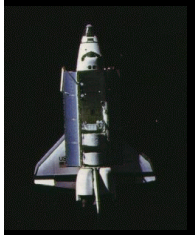
- Displays
  - Crew
  - Ground
- Caution and Warning
- Limit Monitoring
- Event Logging
- Rule-Based Monitoring
- Plots, Trending





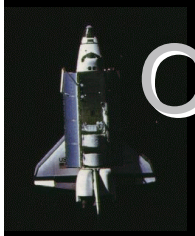






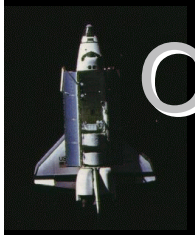
Operations Resources and Tools
Command Capabilities

- Shuttle
  - *Primarily crew-executed through switches and keyboards*
  - *FCT calls up to the crew to executes steps in procedures*
  - *Single FCT commander for systems commanding*
- ISS
  - *Crew and ground command via common computer displays*
  - *Crew typically only works emergency and IFM procedures*
  - *99.9% software controlled*
  - *Distributed FCT commanding*
- Command methods
  - *Manual Commanding*
  - *Scripted commanding*
    - *Onboard (Timeliner)*
    - *Ground*



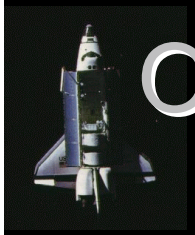
Operations Processes and Techniques
Fault Detection

- Methods
  - *Caution & Warning*
  - *Sensor limit violations*
  - *Trend analysis*
  - *Unexpected response to commands*
- Confirming cues
  - *Use multiple cues to verify accuracy of sensor indications*



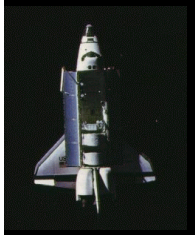
Operations Processes and Techniques
Failure Analysis and Response

- Root cause determination
- Impact analysis – across all systems and activities
- Prioritize multiple failures
- Response determination
  - Identify procedure(s), if applicable
  - Response priorities:
    - Assure health and safety of crew
    - Preserve viability and performance of vehicle
    - Preserve ability to accomplish mission



Operations Processes and Techniques
Post-Failure

- Detailed troubleshooting
- System reconfiguration or IFM
  - Prepare the vehicle to withstand the next possible failure
- Product updates
  - Document anomaly
    - “Failure-Impact-Workaround” format
  - Modify limit sensing values
  - Change procedures to account for new system configuration



Lessons Learned

- Systems Control
  - Flexibility in software design
  - Operations personnel involvement in software development and test
  - Crew and FCT must be able to maintain situational awarness
- Fault Detection
  - Provide sensor validity data with telemetry
- Fault Response
  - System safing responses should be automated
  - Crew and FCT should not be in the critical path
  - Systems should be able to operate in degraded modes
- Troubleshooting
  - Need the ability to downlink more/different data than normally available in telemetry